Developing Cyber Peacekeeping: Observation, Monitoring and Reporting

Michael Robinson[a], Kevin Jones[a], Helge Janicke[b], Leandros Maglaras, Senior Member, IEEE[b,*]

[a] *Airbus, Coedkernew, Newport, NP10 8FZ, United Kingdom*
[b] *De Montfort University, The Gateway, Leicester, LE1 9BH, United Kingdom*

Abstract

Cyber peacekeeping is an emerging and multi-disciplinary field of research, touching upon technical, political, governmental and societal domains of thought. In this article we build upon previous works by developing the cyber peacekeeping activity of observation, monitoring and reporting. We take a practical approach: describing a scenario in which two governments request UN support in drawing up and overseeing a ceasefire which includes cyber terms. We explore how a cyber peacekeeping operation could start up and discuss the challenges it will face. The article makes a number of proposals, including the use of a virtual collaborative environment to bring multiple benefits. We conclude by summarising our findings, and describing where further work lies.

Keywords: Cyber Peacekeeping, Cyber Warfare, Cyber OMR, Cyber Peace Operations

1. Introduction

The United Nations conducts peace operations around the world, aiming to maintain peace and security in conflict torn areas. Whilst early operations were largely successful, the changing nature of warfare and conflict has often left peace operations struggling to adapt. In this article, we make a contribution towards efforts to plan for the next evolution in both intra and inter-state conflict: cyber warfare. It is now widely accepted that cyber warfare will be a component of future conflicts, and much research has been devoted to how governments and militaries can prepare for and fight in this new domain [1]. Despite the vast amount of research relating to cyber warfare, there has been less discussion on its impact towards successful peace operations. This is a gap in knowledge that is important to address, since the restoration of peace following conflict of any kind is of global importance. It is however a complex topic requiring discussion across multiple domains. Input from the technical, political, governmental and societal domains are critical in forming the concept of cyber peacekeeping.

Previous work on this topic has sought to define the concept of cyber peacekeeping [2, 3, 4]. The goal of this paper is to follow up specifically on work by Robinson et al. [4]. We build upon this work by exploring the practicalities of starting up a cyber peacekeeping component and conducting the initial task of observation, monitoring and reporting.

2. Methodology

In Robinson et al. [4], each United Nations (UN) peacekeeping activity was briefly examined for feasibility and value in a cyber warfare context. The aim was to cover the breadth of peacekeeping, and to pick out specific activities which would be both valuable and feasible to perform. This article builds upon this work, by taking the activity of cyber observation, monitoring and reporting (OMR) and discussing how it could be carried out at a practical level. To do this, we also describe the mission start-up process which leads to cyber OMR.

To guide our discussion, we begin by describing a fictional conflict scenario where cyber warfare has been used and is of concern to the involved parties. This scenario is described in section3.

*Corresponding author
Email addresses: michael.mi.robinson@airbus.com (Michael Robinson), kevin.jones@airbus.com (Kevin Jones), heljanic@dmu.ac.uk (Helge Janicke), leandrosmag@gmail.com (Leandros Maglaras, Senior Member, IEEE)

3. Scenario

The neighbouring states of Country A and Country B have a history of conflict, which has traditionally been confined to the domains of air, land and sea. However, in recent months the cyber domain has also been used in a warfare capacity. The cyber warfare aspect of the conflict has included both hard and soft attacks. By "hard" we mean attacks such as denial of service and the planting of malware into sites such as critical infrastructure (power grid, water supply, transport systems etc.). This cyber warfare has been particularly damaging to both sides, interrupting the provision of basic services. Power outages have been common in both nations, and public trust in the water supply is damaged after high profile cases of improper water treatment. "Soft" attacks have included the spreading of misinformation to the public via cyber means and accusations of electoral interference. This combination of hard and soft cyber attacks, has placed both countries on the verge of collapse as a lack of basic services combined with suspicion over the legitimacy of election results has led to civil unrest.

Both countries seek an end to the situation and express a wish for a halt to the conflict. They request UN assistance in drawing up, implementing and verifying compliance with a ceasefire agreement. UN peacemakers begin work to draw up traditional terms such as withdrawal of armed forces to a defined boundary, the holding of negotiations to reach a long term sustainable peace and a process of disarmament by both parties. However, both parties have been significantly damaged by the cyber warfare aspects of the conflict and agree that the ceasefire agreement should also contain cyber terms to end it. Both sides look to the UN peacemakers for leadership and advice in this domain.

3.1. Cyber Peacemaking

In our scenario, both parties look to the UN for assistance in drawing up cyber related ceasefire terms and overseeing their implementation. This will be a new area for the UN, and it is therefore necessary to briefly discuss cyber peacemaking and the kinds of terms which may be agreed upon. The process of mediating and drawing up an effective and lasting ceasefire agreement is a complex and challenging task [5, 6]. A full discussion of this complexity is beyond the scope of this article. Instead, we focus upon the possibilities of cyber related ceasefire terms. This in itself will become a field of research and practice in the future; what we provide here is only the foundation.

A clear starting point for thinking about cyber related ceasefire terms is to propose that both parties cease launching cyber attacks. This aligns with one of the three core ceasefire goals: cessation of hostilities [7]. In practice such a term would be difficult to monitor due to the problem of attribution in cyberspace [8]. As discussed in Robinson et al. [4] and in many other works [9, 10], this is the technical challenge of gathering unequivocal proof that cyber attack X came from party Y. In short, it is difficult to present proof that would pass even the minimal of evidentiary standards [10]. This is not particularly a problem for nations; they are free to attribute attacks without fear of having to reveal their sources or open their evidence to independent inspection. This leads to what has been named faith-based attribution: nonscientific analysis that leads to untestable attribution [10]. UN peacekeeping cannot and should not employ such methods. It is an activity based upon the trust of both parties and transparency. It is therefore essential that claims of ceasefire violations must be backed up by open evidence. It has consequently been argued that peacemakers should simply avoid any cyber terms which require solid, verifiable attribution [4].

This conclusion limits the types of terms which could be included in a cyber ceasefire agreement. For the purposes of our scenario, we can take the examples given by Robinson et al. [4], and add one more:

1. Both countries to provide full assistance to UN cyber peacekeepers in dismantling botnets and other sources of denial of service attacks which are physically located in their borders.

2. Both countries to cooperate with the UN in the prevention of cybercrime/spoiler attacks which are originating from within their borders.

3. Declaration of information stolen during the conflict.

4. Declaration of systems compromised and assistance with returning control to rightful owners. Caution must be used here because there may be a dispute about who the rightful owners of certain systems are.

5. Declaration of known vulnerabilities in critical infrastructure.
6. Remote disabling of malware (if possible) or assistance in locating and removing malware.
7. The right for each party to request UN cyber peacekeeper monitoring of particular sites.

These ceasefire terms avoid the attribution problem because they all involve person to person cooperation that can be observed and monitored. Peacekeepers can observe how cooperative each party is in helping to dismantle botnets, disable malware, return control of systems and declare vulnerabilities. Regardless of the result of such cooperation, clear demonstrations of transparency, honesty and openness in assisting cyber peacekeepers would be seen as fulfilment of the agreement. Conversely, inaction, opaqueness or refusal to cooperate can be indicators of a violation. Measuring the levels of compliance in this way will be much more productive to peace and a better use of resources in comparison to engaging into debates about proof with each party. It must be noted that choosing to sidestep the challenge of attribution does not mean cyber peacekeepers will simply ignore the problem of cyber attacks. As will be discussed, they will be handled in a defensive manner.

It is noted that these are a simplification of ceasefire terms. As noted in ceasefire literature [11, 7] there is no room for ambiguity, and every term such as denial of service, botnet and cyber-crime must be clearly defined and agreed with both parties. The terms presented here are therefore just examples, chosen for the purposes of describing how cyber OMR could be performed.

4. Mission Start-Up

With a ceasefire in place, the UN Security Council is in a position to authorise a UN peacekeeping operation which contains a cyber component. We therefore explore the practicalities of starting up the cyber component of such a mission. Whilst UN processes are complex, we propose that a cyber component can fit into existing processes without the need for any significant changes to the established ways of working. This is because the processes themselves have been designed with the aim of unifying multiple disparate entities. We begin with a discussion on securing the necessary cyber expertise.

4.1. Finding Cyber Expertise

Our scenario represents a situation the UN may find itself in: being asked to guide the drawing up of a ceasefire agreement which meaningfully addresses cyber warfare and overseeing its implementation. If unprepared, the UN may struggle to secure the expertise at short notice, leading to delays in the peace process. This is undesirable as once started, a peace process must progress quickly to capitalise upon the honeymoon period [12]. Similarly, securing the wrong types of expertise may lead to failed implementation and a relapse into conflict. It is therefore essential to think about how the UN could secure suitable cyber expertise ahead of time. To assist with this task, we first describe how the UN secures expertise presently.

The UN has no standing army or police force, and must request contributions of troops, police and observers from UN member states who act as Troop Contributing Countries (TCCs) and Police Contributing Countries (PCCs) [13]. As of February 2018, the UN had just over 100,000 contributed police, military experts and troops from 123 nations [14]. Although the word contribution suggests that they are charitably donated, nations contributing troops are reimbursed at a standard rate, which in 2018 is US$1,332 per soldier per month [15]. Numerous works exist which explore why states do or do not choose to contribute personnel [16, 17, 18].

The UN also maintains a pool of civilian staff. As of 2018 the UN had more than 15000 civilians serving in peacekeeping operations around the world [19]. These civilians fulfil many roles not suited to either troops or police, such as providing general administrative assistance, acting as public information officers or providing specific expertise such as logistics or ICT knowledge. Civilians can serve as international staff, national staff from the host country, as UN volunteers, consultants or contractors [19].

Clearly the UN already has the systems in place to acquire expertise from multiple sources: it can tap into national militaries and police forces around the world or from civilian sources where necessary. When considering cyber peacekeeping, we propose that cyber expertise could come from all of these sources. States can be a source of cyber peacekeepers by contributing military cyber warfare troops and cyber crime police officers, but expertise can also be found in non-governmental organisations, private industry, charities and volunteers. It is

therefore possible to define multiple sources of cyber peacekeepers:

- Cyber Contributing Countries (CCCs) - States which contribute uniformed cyber peacekeepers from the police or military.
- Cyber Contributing Organisations (CCOs) - Organisations which contribute civilian cyber peacekeepers from their workforce.
- Volunteers - People with cyber expertise who volunteer their time.
- Full time UN cyber staff - civilians recruited as employees by the UN.

Aside from these traditional approaches to securing personnel, there is ongoing debate regarding the use of private security companies (PSCs) in UN peacekeeping operations. The use of private security companies in conflict areas is not new, with companies such as Blackwater providing armed security in Iraq [20]. To date, the UN has avoided using PSCs for front line activities, but has contracted companies such as ArmorGroup for mine action duties with successful results [21]. With a willingness to use PSCs, their potential as a reliable source of cyber peacekeepers is clear but caution must be used since the disadvantages of PSCs are well documented [21].

An advantage the UN has in searching for cyber expertise is that cyber peacekeepers will be required in much lower numbers than troops or police. While a border may require thousands of troops to guard and patrol it, a network can be monitored by a handful of cyber peacekeepers, utilising technology to automate a number of monitoring tasks. This lower number of required staff will slightly mitigate the many problems described next.

Although there are many potential sources of cyber peacekeepers in theory, they will likely be challenging to secure in practice. The reasons for this are political, societal and economic in nature. To begin, we briefly discuss the existing challenges of securing troop and police contributions.

The problems faced by the UN in securing good quality contributions is well documented [22, 23]. Nations with highly trained troops and police are unwilling to face a shortage at home by sending them abroad to potentially dangerous regions [16]. Those nations with inexpensive personnel are more likely to contribute, but the incentive here is often economic: the compensation provided by the UN per soldier or officer is often more than their cost [16]. For example, some of the most significant contributions have come from nations such as Bangladesh, Pakistan, India, Nigeria and Ghana [16]. The US, UK, France, China and Russia all have a record of low personnel contributions to UN peacekeeping missions [16]. Whilst economics plays a part in this discrepancy, it is not the only factor. The decision on whether to contribute can depend on many factors such as if it is in their own national interest (e.g. the instability is on their border and could spillover) and the level of toleration for casualties (the US withdrawal from Somalia in 1994 was partially due to a low tolerance for the loss of US troops) [18].

When looking to the cyber domain, we must navigate these factors to evaluate how likely contributions of cyber personnel will be.

From an economic perspective, the indicators are not good. As the threat of cyber warfare increases, nations are competing to secure good quality cyber expertise in a market with limited supply. In 2015 it was reported that the US Cyber Command only has half the staff required, citing competition with the private sector as an obstacle towards securing the staff numbers it needs [24]. With nations and businesses around the world competing for a limited supply of good quality cyber personnel and incidences of cyber warfare and crime increasing, cyber peacekeepers will be an expensive asset.

Looking from a political angle, the willingness to suffer a cyber skills shortage at home for the benefit of UN peacekeeping abroad is likely to be limited. Even if a highly cyber developed nation could technically spare cyber personnel, it is debatable whether they would allow their staff to work alongside staff from another cyber competing nation. This is significant in a political environment where tensions over cyber warfare currently run high between some of the most cyber developed nations [25, 26]. Nations may prefer keep their cyber personnel at home, or to limit sharing with trusted partners such as NATO or the African Union.

Although there are clear challenges, some aspects may encourage contributions. For example, proximity to the conflict area may be a driver of cyber peacekeeper contribution: critical infrastructure at risk of failing could potentially impact neighbouring states. In this regard, there is a self interest to contribute the expertise. Furthermore, it has been noted in the literature that peacekeepers of-

ten stand to benefit professionally from the experience [27]. Peacekeepers also largely report their duties to be satisfying [28] and studies have shown that the experience of peacekeeping has a beneficial effect on quality of life [29]. With this in mind, cyber peacekeeping may be attractive to civilians who are looking for both job satisfaction and a level of professional development that otherwise might not be open to them.

Although the UN will be aiming to secure relatively small numbers of cyber peacekeepers, the issues described will be a significant challenge. Nations may be unwilling to contribute personnel and it remains to be seen how much civilian interest will emerge. This challenge cannot go ignored, and methods to encourage contributions and civilian recruitment must be built into the design.

4.2. Fitting cyber into the organisation

While securing cyber talent will be challenging, we assume that the UN will be able to secure some. With this assumption, we must next consider how these cyber staff will be organised, and where they will be placed into the existing organisational structure. Figure 1 shows a simplified version of the existing structure:

At the tactical level there are currently military, civilian and police components. Each of these units is overseen by a component head who reports to a leadership team at the mission headquarters. At the tactical level, an immediate question becomes apparent: should cyber peacekeepers be considered as military, police or civilian units?

Based on our discussion in section 4.1, we have already proposed that cyber peacekeepers will come from multiple sources: some will be from the military, some from police forces and some from civilian backgrounds. One approach would be to simply assign cyber peacekeepers to the unit which matches their background. For example, a cyber peacekeeper from a national military would be assigned to a military unit whilst civilians would be assigned to a civilian unit. This approach does have its advantages (for example, a military cyber peacekeeper could potentially be armed and supported by infantry) but it would also potentially damage communication and coordination between cyber peacekeepers. We therefore propose that due to the unique nature of cyber peacekeepers, a new type of unit is created: cyber units. Placing cyber peacekeepers into a cyber unit would facilitate cohesion, regardless of their source. It would also

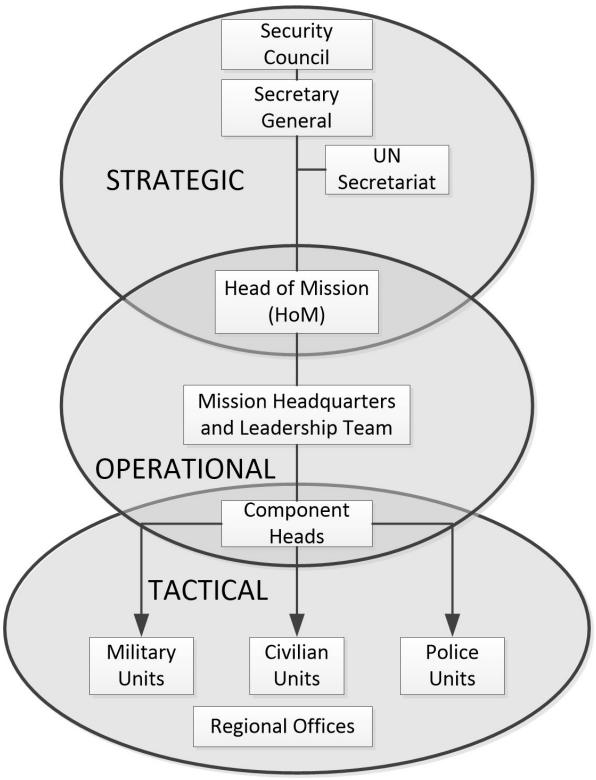

Figure 1: Traditional UN Peacekeeping Organisational Structure

open up a new role, the head of cyber component, to oversee and be responsible for the tactical cyber aspects of a particular operation. Figure 2 shows where a cyber component would fit into the organisational structure.

Whilst the head of cyber component will report to the leadership team and head of mission for operational planning and reporting, it is envisioned that cyber experts will also be present at the strategic level to guide decision making in strategic aspects relating to cyber.

4.3. Mission Planning

The overall planning process for UN peacekeeping operations is complex, consisting of multiple plans and processes[30, 31]. A simplified overview of the plans that need to be developed and their hierarchy in relation to each other is shown in figure 3.

Laying the foundation for other plans, the Security Council mandate sets out an overall political goal. In our scenario, this would be to secure peace between the two countries. This mandate is then

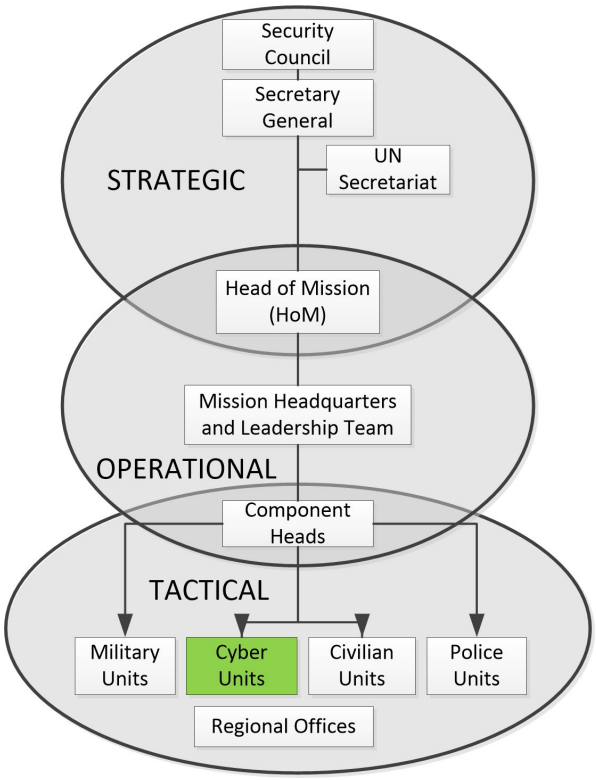

Figure 2: Proposed UN Peacekeeping Organisational Structure (Cyber Units Added)

used to formulate a country wide plan: for example, what is required in Country A to fulfil the mandate. Mission wide plans then define how these political intents can be reached at the strategic level, giving statements on the type of activities that will be required. Finally, the component level plans use the mission wide plans to formulate plans at the tactical level: specific actions, time lines, expected outcomes and so on. In the next section, we explore how such a component plan could look for a cyber unit in Country A.

5. The Cyber Component Plan

In our scenario, the cyber component plan would set out the high level objective of the cyber component: to support the Security Council mandate by providing the cyber capability that is necessary to support the restoration of peace. In particular, the priority of the cyber peacekeeping unit (CPU) will be to ensure compliance with the cyber terms in the ceasefire agreement. This high level objective will then be broken down into smaller tasks,

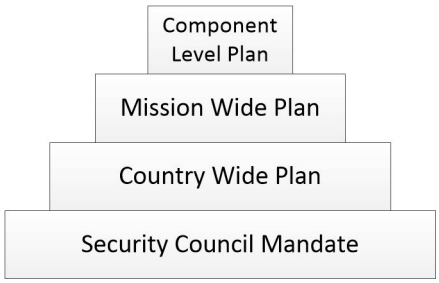

Figure 3: UN Peacekeeping Plan Levels

such as conducting technical assessment missions on proposed sites, forming links with local stakeholders and building an observation, monitoring and reporting capability at sites where the value towards maintaining peace is high.

5.1. Technical Assessments

One of the terms in our ceasefire agreement is the right for each party to request UN cyber monitoring of particular sites. Country A requests monitoring of:

- The president's office.
- The power grid.
- The control system for their flood defences.

These requests are initially made to UN peacemakers, but are passed to the head of cyber component for expert evaluation. The head of cyber component considers the requests and launches technical assessment missions to evaluate which to grant. Such assessments are not new to UN peacekeeping. They are already well established in peacekeeping as a means to evaluate the feasibility and value of carrying out a particular task before it is agreed to. The UN planning toolkit [32] provides guidance on how such assessments should be conducted. From a cyber component perspective, these assessment missions should evaluate:

1. The specific ways in which monitoring this site would contribute towards peace (e.g. a cyber attack upon the site could threaten civilian lives or lead to state collapse).
2. The level of local support: do local staff welcome the cyber peacekeepers and cooperate? Are network diagrams made available for inspection and are staff forthcoming with assistance?

3. Capacity to act: can the site be effectively monitored given the current funding, availability of cyber expertise and equipment?

In practice this assessment would likely find limited value in monitoring the president's office and this request would be denied; however, for the purposes of describing how to conduct cyber OMR in its simplest form, it is a useful example. This is because the president's office is a traditional ICT environment characterised by desktop computers, mobile devices, printers, databases and so on. It is this kind of environment in which the majority of cyber security literature and understanding is based. We will therefore assume that the request was granted and describe how a cyber OMR capability would be established in an ICT environment such as the president's office.

6. Cyber OMR in ICT environments

From the conclusions made in Robinson et al. [4], combined with our scenario's ceasefire terms, it is possible to be concise about what cyber OMR is trying to achieve in our scenario:

- Detecting actions which violate the ceasefire agreement - our ceasefire terms were chosen to avoid attribution and to be monitorable through social interaction.
- Detecting violations of human rights - In our scenario this is primarily protecting civilians from harm (e.g. the right to life).
- Detecting changes in network structure and network traffic - by itself this does not bring direct value, but supports the other goals by raising situational awareness at a network.

The first goal does not require any technical discussion: peacekeepers already observe levels of cooperation and compliance and this happens on an interpersonal level. Where more discussion is required is in regards to the second and third goals and the necessity to establish a technical monitoring capability at agreed sites.

6.1. Establishing a monitoring capability

Just as military units will look to establish an effective observational capability through the use of patrols, observation posts and checkpoints [33], cyber units will look to establish an effective observational capability through cyber means.

The monitoring of computer networks is a well established domain of cyber security. We can therefore look to existing literature and best practice for guidance on how we could establish this capability in a peacekeeping environment. For example, we can turn to guidance from authors such as Bejtlich [34] on how to establish suitable network security monitoring solutions in a traditional ICT environment.

This will initially involve a planning stage, where cyber peacekeepers consult with local staff and build a picture of the network, the information expected to be flowing in and out and any existing monitoring solutions. In line with established doctrine, the emphasis in cyber OMR should be to engage local stakeholders such as IT staff and support them with the cyber knowledge, expertise and equipment they may lack, rather than taking over the site and dictating actions. In our scenario, the UN is operating with consent of the host nation and all involved parties. Additionally, technical assessment missions have already concluded that local staff are willing to assist and are ready to engage with the process.

If discussions lead to the conclusion that existing sensor coverage is insufficient, new sensors should be placed into the network to fill gaps in visibility. These sensors can be network taps (dedicated devices added onto the line to intercept all traffic) or span ports at existing network devices (a port which replicates all data passing through a switch).

Once cyber peacekeepers and local staff are satisfied that monitoring coverage is sufficient, they can begin to monitor the network and report upon events which may impact the security of civilians. The technical methods of interpreting the captured data is an established field of study, and cyber peacekeepers will be expected to exercise and share their expertise of network security monitoring here. Numerous sources of guidance and best practice exist [35, 36, 37], as well as various off-the-shelf software tools such as Security Information and Event Management (SIEM) products and packet sniffers. Cyber peacekeepers will use their expertise to determine which tools will be best for the particular environment they are working in.

The key ingredients to success in this scenario are two-fold: the ability for cyber peacekeepers to build up rapport with local staff and for them to gain a familiarity with the network they are monitoring.

Where networks are small, this is not likely to be a problem. Where a network is larger or highly geographically dispersed, these two goals will be harder to reach. When considering systems such as the power grid, components can include power plants, transmission systems, distribution substations and more. We must consider ways for a cyber peacekeeping unit to gain familiarity across such large sites both technically and socially.

We propose that the concept of areas of responsibility from existing peacekeeping documentation can be leveraged for this task. Areas of Responsibility (AoRs) is a term used by UN infantry battalions to divide a geographical area into smaller areas for groups of infantry to patrol and observe [33, 38]. This makes it easier for commanders to assign troops efficiently and ensures that necessary areas are covered by the right amount of manpower. It also allows the building of trust between peacekeepers and local people, due to the opportunity to build up familiarity over time and develop an appreciation of local issues. It is proposed that the concept of AoRs would be suitable for cyber OMR, since it would allow cyber peacekeepers to focus on one area of the site. The benefits of using AoRs are summarised as follows:

- Splits the observational workload into manageable sub-areas.
- Allows a team to build up familiarisation with the network area they are monitoring (its structure, traffic patterns etc.)
- Enables a team to build rapport with local staff on that part of the network.
- Allows cyber peacekeepers with different areas expertise to focus on specific systems.

In the case of the power grid, a simplistic view of AoRs being leveraged is visualised in figure 4. In the figure, we see that multiple parts of the power grid have been split into observation areas. Cyber peacekeepers with expertise in industrial control systems (ICS) can therefore be assigned to the generation or transmission AoRs, whilst those with more expertise in traditional ICT environments can be assigned to the office or control centre. Once assigned, these staff will then be able to build up familiarity with both the systems they are monitoring and the local staff.

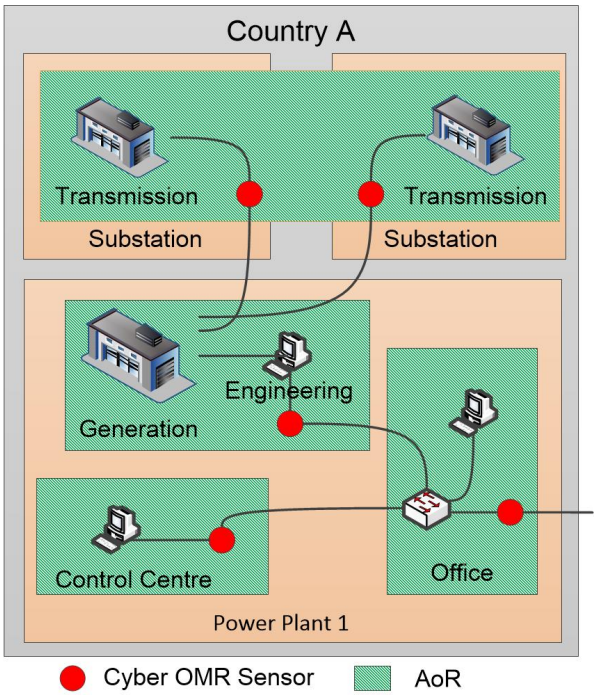

Figure 4: Simple representation of areas of responsibility in cyber OMR

6.2. Monitoring of an AoR

With the establishment of AoRs at monitoring sites, cyber peacekeepers now have a technical capability to perform cyber OMR. The next step is to consider how cyber peacekeepers use this capability to produce value for a peacekeeping operation. It is proposed that there are two approaches towards the observation and monitoring of an AoR: local and remote.

6.2.1. Local

The local approach involves cyber peacekeepers travelling to the AoR and performing their duties in person. The advantage to this approach is that cyber peacekeepers will be able to build up a face to face relationship with local staff. This facilitates trust between cyber peacekeepers and local stakeholders, which is regarded as vital to the success of any peacekeeping operation [38]. Local cyber peacekeepers can also maintain the sensors as required. The disadvantages of the local approach are numerous however. Firstly, cyber peacekeepers would have to physically travel to the site; finding cyber peacekeepers who wish to relocate may be difficult. At a personal level, the physical security of

the location may be questionable, and work or family commitments may prevent it. This may result in reduced civilian recruitment. At an organisational level, the challenges regarding the global shortage of cyber personnel discussed in section 4.1 may mean that governments and organisations are reluctant to be without cyber staff whilst they travel to a foreign country. This issue has already been encountered by the UN in regards to securing police contributions [22].

It must be noted that the local method may be the only option available in certain cases. For example, in cases where air-gapping theoretically exists, external connections may be prohibited and/or unavailable. Similarly, the technical assessment missions and deployment of additional sensors if needed would further necessitate a local approach.

6.2.2. Remote

The second approach is the remote method, which capitalises upon an attribute of cyber warfare: lack of geographical restriction [1]. Once a technical assessment mission has been completed locally and a monitoring capability established, it is envisioned that some monitoring could be performed remotely. Sensors at the site can report back to a central server, whereby analysis of the collected data can be performed from any geographical location.

The advantages here are numerous and significant. From the perspective of a contributing government or organisation, cyber experts they contribute are not being completely surrendered. Contributors can agree to donate a limited portion of a cyber expert's time per day, the majority still being available to the contributor. This is a significant benefit for the UN when trying to secure the necessary cyber talent in a highly competitive global market: if contributors are not losing access to the cyber expert, they will be more likely to contribute. From the perspective of the cyber peacekeeper, the concern of physical security is also removed, and there is no need for the UN to fund the accommodation and living costs associated with the local approach.

The remote approach is not without disadvantages. Even if the cyber peacekeeper is fully vetted and determined to be non-malicious, there is a risk when allowing cyber peacekeepers to perform their duties remotely with their own hardware. For example, there is the potential for their system to be infected with malware which can lead to breaches of security. To mitigate this issue, the UN may opt to send cyber peacekeepers a hardened, locked down and monitored system which is used purely for the purposes of cyber peacekeeping. Similarly, the UN would be relying upon the public internet and peacekeeper's own internet providers to conduct cyber OMR. At critical sites with the possibility of significant harm to civilians, this risk may be too high. A possible mitigation of this risk would be to use a dedicated communications network. Another disadvantage is that by being remote, there is potential to lose the face to face collaboration and rapport building that comes with the local approach. To resolve this concern, it is proposed that a virtual collaborative environment (VCE) could be used.

6.3. Virtual Collaborative Environment

Virtual collaborative environments are digital spaces where remotely located people can come together and interact with each other and with virtual objects. The benefits of VCEs are well established [39, 40] and research into new applications for VCEs in areas such as science, education and business is ongoing [41, 42].

From a cyber peacekeeping perspective, potential off-the-shelf options include Vastpark, Protosphere, Second Life, Opensimulator and Open Wonderland. Market reviews and research which describe the features and capabilities of these software options are available [39, 43]. A further option is for a custom solution to be developed using an engine such as Unity [44]. It is proposed that any VCE used by cyber peacekeeping must fulfil the following non-functional requirements:

1. Scalable - The VCE should be suitable for both small and large scale cyber peacekeeping activities, and allow for changes in scale without disruption to the operation.

2. Robust - The VCE must be reliable, accepting a high number of concurrent users with no failures of availability. Considering the nature of cyber peacekeeping, it must also be secure from cyber attacks such as denial of service and man in the middle attacks.

3. Secure - Sensitive information will be contained in the VCE. It must have access control, secure communications and auditing features.

It must also fulfil the following functional requirements:

1. Resource sharing - Cyber peacekeepers will need to examine sensor data together and study information from a variety of sources inside the VCE.
2. VOIP - Allowing cyber peacekeepers to communicate with each other and local stakeholders in real-time.
3. Reporting - The reporting system should be available from inside the VCE.

In line with the goal of this paper to provide practical guidance, we developed a proof of concept VCE. OpenSimulator was chosen for this since assets were readily available online and the set-up process was straight forward. A basic world was built using terrain found at the OpenVCE website [45].

Defining the requirements of a cyber peacekeeping VCE allowed the drawing up of potential layouts. Figure 5 shows the first design of a cyber peacekeeping VCE. The Type 1 VCE is a simple layout whereby each AoR has a monitoring area, showing the sensor data and other information in real-time to cyber peacekeepers. Cyber peacekeepers can log in to the system from anywhere in the world, gain access to the sensor data and communicate in real time with other cyber peacekeepers and stakeholders. The Head of Cyber Component (HoCC) and his or her team is also present in the VCE if needed (for example, in times of crisis). This infrastructure allows all parties to achieve situational awareness, communicate with each other in real time, cross correlate events and provide assistance or inspect incidents as they happen. Local stakeholders are invited into the environment to communicate, contribute and witness how the monitoring is progressing. This encourages transparency in the operation and fosters trust. Liaisons from other unit types such as police and military can also be present, allowing for timely and unified coordination of actions across the whole operation. Note that cyber peacekeepers are not strictly confined to their station, and may assist and communicate freely with other people as needed.

There are advantages and disadvantages to the Type 1 layout. On the plus side, it is a simple design which fulfils the previous criteria. All AoRs are monitored and staff can communicate and assist each other freely. Arguably the most significant disadvantage is that it is resource intensive

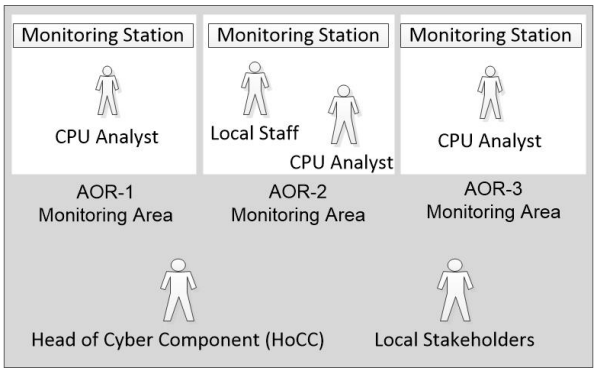

Figure 5: VCE Layout Type 1

and fatiguing for staff. Using this design, each AoR is manned 24/7 with cyber peacekeepers being required inside the VCE and performing real time monitoring. This observation therefore raised the question of whether the monitoring needs to be real time or if it can be performed in batches (for example, reviewed every X hours).

To answer this question, we turn to existing cyber security literature. Bejtlich [46] states that the decision to use real-time or batch analysis during network security monitoring primarily depends upon management's expectations on timeliness of reports. This is a reasonable stance, since in a private organisation it is management who balance up the risks versus costs and reach a conclusion that suits their organisation. Peacekeeping is different; there are multiple stakeholders who each have their own expectations of what the operation should deliver. Taking our scenario, Country A might be satisfied with daily reports containing summaries from the previous 24 hours. Country B might have different expectations, and expect to be informed the moment a violation is detected. Local variations may exist such as the the power grid demanding daily reports whilst the operator of the flood defences may desire them every four hours. There are also additional considerations such as the potential for civilian harm if an attack is not observed quick enough. In this regard, peacekeepers themselves may have their own view on how regularly data should be reviewed. The pros and cons of real time and batch monitoring during cyber peacekeeping are shown in figure 6.

The major advantage of real-time monitoring is that safety critical events can be detected quickly. Although OMR is a passive activity in both kinetic and cyber peacekeeping, it has been repeatedly em-

	Advantages	Disadvantages
Batch	More efficient use of expensive resource (cyber peacekeepers) Less demand on contributing parties (can be fixed contribution of time/day)	Potential delay in detecting and reporting of events which may threaten civilian security
Real Time	Potential to detect civilian threatening events quicker	Full time cyber peacekeepers required (expensive) Increased demand on contributing parties (cyber staff donated for more hours)

Figure 6: Real-time vs. Batch Monitoring

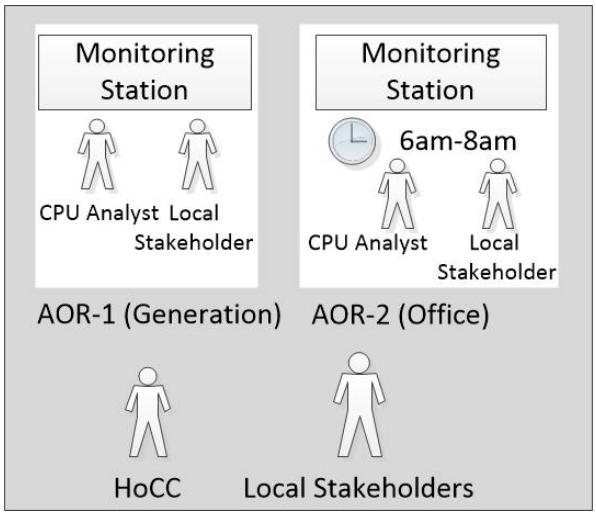

Figure 7: VCE Layout Type 2

phasised that impartiality does not mean neutrality [47]. UN peacekeepers have a duty to intervene if they witness and are able to prevent a threat to the security of civilians [13]. This is a compelling justification for cyber OMR being real time, particularly on safety critical networks such as air traffic control, dams, and nuclear facilities. This must be balanced against the personnel issues raised in section 4.1: cyber expertise will be expensive to secure, civilians will be difficult to recruit and contributing nations may be reluctant to contribute staff if they are required for extensive periods of time.

Looking at the arguments for and against, it is concluded that cyber OMR should use both real-time and batch monitoring. Batch monitoring should be the default choice, but technical assessment missions can recommend real-time if it is necessary to prevent harm to civilians or the wider peace process (e.g. potential for state collapse or destabilisation). Relating this back to our scenario, the technical assessment mission at the power grid has concluded that whilst the generation AoRs will require real-time monitoring, the office would be suitable for batch monitoring every 24 hours. Figure 7 shows how this could be organised in the VCE.

Here cyber peacekeepers are providing real-time coverage to AoR-1, along with others who log in every 24 hours and perform batch monitoring in pairs for a period of two hours. This pairing of staff allows them to discuss alerts and events between themselves before raising a report up the command chain. It is less resource intensive, with the cyber peacekeepers and local staff only being required for the time it takes to work through the events from the previous 24 hours.

The significant benefit of this approach is the minimisation of the time required from cyber peacekeepers. By using batch monitoring where possible the UN is not only seeking to minimise the number of cyber peacekeepers required, but also the amount of time they are required for. The time commitment of two hours per day is only an example, and in reality will vary depending upon the complexity of the AoR. The attraction of this limited time period is that public and private organisations can contribute cyber staff with only a minor impact to their own operations. While this would not guarantee contributions, it would arguably make them more likely.

A proof of concept Cyber OMR VCE was created using OpenSimulator, following the design given in figure 7. Figure 8 shows the result. The environment is split into six areas, each one being an area for an AoR team.

The VCE allows cyber peacekeepers and local stakeholders to log in and be represented as an avatar. They are able to communicate with each other via voice and text and to bring up data on the three displays for interaction and discussion. In our example, these screens link to the AoR sensors and display sensor data. An example of this is shown in figure 9. In practice, these displays can be used for sharing any kind of data to aid in discussion and analysis. In effect, it is a virtual security operations centre (SOC) but one that can be quickly deployed

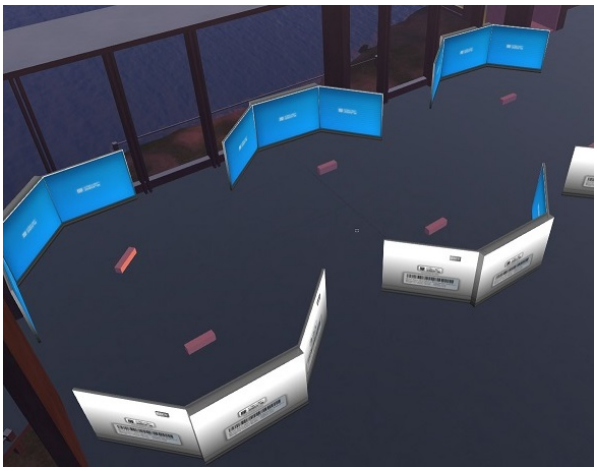

Figure 8: PoC VCE Layout

and used by multiple remote analysts.

Figure 9: PoC VCE Resource Sharing

Whilst we have proposed that a VCE is used to mitigate the challenge of securing cyber staff contributions, we have noted that it brings other benefits. These benefits are summarised as follows:

1. Encourages cyber staff contributions - Nations will be more likely to contribute cyber expertise if that expertise will not be lost at home. Contributions of time can be a fixed amount of hours per day.

2. Transparency - Cyber peacekeepers can be open in their activities by inviting local stakeholders into the environment to witness their work.

3. Mission cohesion - The VCE brings all cyber peacekeepers in a region together, allowing cross correlation of events and sharing of expertise. Non cyber units can also be present, to aid mission wide cohesion, communication and unity of effort.

4. Agility and Cost - The VCE can be brought online with minimal cost. There is no need to house or feed remote cyber peacekeepers.

5. Safety - Remote cyber peacekeepers in the VCE cannot be physically harmed.

6. Training - New cyber peacekeepers can be vetted and trained inside the environment.

Considering all of these advantages, it is concluded that the VCE will bring benefits beyond just OMR. It will therefore become a central tool for conducting multiple aspects of future peace operations.

6.4. Secure Communications

In the case of remote cyber OMR, the sensors will be located locally in the conflict area whilst those analysing the data will be located remotely. A secure means of transferring the data collected by sensors to the central server and subsequently into the VCE is therefore required. Similarly, in the case of the local approach, locally based cyber peacekeepers will need a secure channel to transmit their reports.

Due to the nature of cyber warfare, we cannot automatically assume that the technology and infrastructure we rely upon to perform this task will be secure. Hardware, software and public communications networks could potentially be compromised [48]. In cases of ongoing cyber attacks, networks could be flooded with traffic and routing systems compromised [49]. It is therefore proposed that a cyber peacekeeping unit will require a robust set of technologies to mitigate these issues.

To begin, a dedicated and mobile communications link which is difficult for third parties in a region to tamper with will be required. A potential solution here would be the use of satellite services. For example, the Broadband Global Area Network (BGAN) offered by Immmarsat [50] can provide cyber peacekeepers with speeds of up to 492kbps.

Coverage is close to global and the terminals are approximately laptop size and weight. This solution would create a reasonably secure communications path for cyber peacekeepers to operate inside a region and perform their duties, regardless of the condition of local networks. Research into the security and privacy of mobile networks is an ongoing area of study and developments here can also bring solutions [51]. We must also consider the hardware used by cyber peacekeepers; components such as CPUs and motherboards also have the potential to be compromised along the supply chain [48]. This is a much harder threat to mitigate, and is a common problem. For example, in 2010 Dell Power Edge 410 servers were shipped with malware pre-installed on the motherboards [52]. Establishing a secure supply chain will consequently be a challenge faced by a cyber peacekeeping unit.

6.5. Proof of concept tools

We have purposely avoided listing specific tools that cyber peacekeepers should use to perform OMR and there are two primary reasons for this. Firstly, cyber security tools are always evolving, and any list provided here would be quickly out of date by the time cyber peacekeeping is needed. Secondly, cyber peacekeepers are being employed for their expert knowledge, and should be allowed to select the tools and monitoring methods that suit their specific site. However, for the purposes of exploring the practicalities of cyber peacekeeping OMR, we briefly experimented with potential tools that could fulfil the cyber OMR goals of our scenario.

To recap, the value we aim to bring is in detecting actual or impending threats to civilian security. In the case of the power plant, this could be through a power cut, power surge or a violent event such as an explosion by tampering with the logic that runs the plant. Achieving this goal will be supported by monitoring for changes in network structure and traffic (i.e. raising situational awareness in an AoR).

In our proof of concept environment, we already have sensors collecting data and a VCE to view and analyse the results. We considered ways to monitor the network structure, and found that commonly available tools such as Alienvault OSSIM had functionality to monitor the availability of hosts. When a particular host was taken down, alerts could be raised and viewed in the VCE. Important structural devices such as routers and firewalls could be configured to send their logs to the SIEM and custom rules developed to monitor for changes. Hence, any changes to the network structure could be highlighted in the VCE, allowing analysis of the change. Other tools such as the Passive Real-time Asset Detection System (PRADS) can also be used to monitor for new devices or changes in known asset behaviour [36].

Similarly for changes in network traffic, we were able to configure NetFlow [53] on the sensors. This allowed analysis of the network traffic volume over time. An example of a simulated change in network traffic is shown in figure 10.

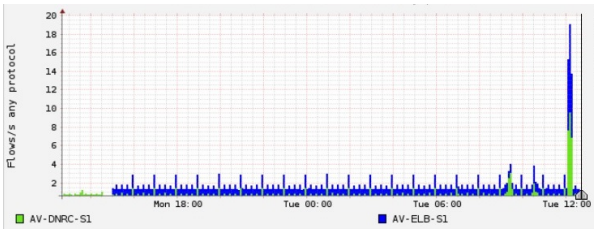

Figure 10: Detecting a change in network traffic volume

While it is beyond the scope of this article to compare and test specific monitoring tools, we have shown that there are many practical tools to perform the technical aspects of cyber OMR in an ICT environment if it was required today. Where more of a challenge will be found is in operational technology (OT) environments such as critical national infrastructure.

7. Cyber OMR at Critical National Infrastructure

The methods and techniques described thus far will be effective in a traditional ICT environment such as the president's office scenario. Where monitoring becomes more challenging is in OT environments such as critical national infrastructure (CNI). Power grids, public water supplies and transport networks will be commonly requested sites for cyber OMR. This is because attacks upon these systems present a significant threat towards life and to the ongoing stability of a nation. In this section, we therefore describe the characteristics of CNI from a monitoring perspective, the challenges that will be faced and ways to tackle those challenges.

7.1. CNI Background

The UK government defines national infrastructure as the "facilities, systems, sites, information,

people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example)." [54]. Figure 11 shows which sectors are identified by the UK as national infrastructure:

Chemicals	Civil Nuclear Communications	Defence
Emergency Services	Energy	Finance
Food	Government	Health
Space	Transport	Water

Figure 11: Areas the UK regards as National Infrastructure

Critical National Infrastructure is defined as: "Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life." [54]. This definition supports our assertion that CNI will be a popularly requested site for cyber peacekeeping, since failure directly impacts peace and security.

Research into the cyber security of CNI and the challenges it presents is extensive [55, 56, 57, 58]. Piggin [59] provides a concise overview of the potential impacts and attack vectors, but it is prudent to give a brief history and overview of the main challenges, to enable discussion on how to conduct cyber OMR at such sites.

National infrastructure of the past was generally isolated from the outside world, operating as standalone entities with no external connections [55]. In this isolated environment, the threat of an external actor performing some kind of malicious act was small. Hence, the availability of the systems was the top priority, with confidentiality and integrity being less important. The protocols used between devices at such sites (Modbus, DNP3 etc.) reflected this: encryption was rare and communications were not tamper resistant [60].

With the arrival of affordable computing and networking, owners of these facilities saw benefits in connecting them together. Rather than employ staff to monitor a single facility, geographically distributed plants could be monitored and operated from a central location using Supervisory Control and Data Acquisition (SCADA) systems [55]. This provided a greater level of control with improved efficiency. Today, national infrastructure capitalises on many modern technologies including mobile networks, wireless communications, the internet and embedded devices [60, 61]. Whilst the technology used at CNI can be referred to by a number of terms, we adopt the umbrella term of operational technology (OT).

Whilst the OT used in CNI has enjoyed improved connectivity and efficiency, it has effectively been wrapped around legacy protocols and devices that have remained unchanged from the days of isolation. This has created the perfect storm of introducing multiple vectors of attack into systems which generally have poor security features.

7.2. Challenges of cyber OMR at CNI

We have argued that CNI will be a significant part of cyber OMR for a number of reasons. Firstly a failure of CNI has the potential to seriously damage peace and security in a region through harmful impacts [59]. These impacts can not only include immediate physical harm, but also cascading damages from outages of critical services [62] which governments are not necessarily prepared for.

CNI is also particularly vulnerable to cyber attack due to increased interconnectedness and weak security at core components. From a governmental perspective, it is also challenging to gain a reasoned understanding of the true threats [63]. This makes a cyber peacekeeping force well suited to operating in CNI, and we must therefore explore how cyber OMR could effectively monitor such sites. From the perspective of conducting OMR, we propose that cyber peacekeepers will face the following CNI specific challenges:

1. Fragility - older OT hardware can be fragile [64]. Software used to program ladder logic can be basic with poor error handling. A network port receiving unexpected data can cause a hardware reset, in some cases causing a loss of the device's current logic. Research has shown that tasks such as asset discovery can only safely be performed via passive methods [65].

2. Bespoke attacks - Sensors on traditional ICT networks use signature based detection to identify known attacks. While this technique will

detect some attacks against OT systems (particularly machines running common software such as Microsoft Windows or Java), it will not help in cases where there is a targeted attack against specific OT hardware. Stuxnet was a bespoke cyber weapon crafted specifically for attacking Iranian nuclear facilities [66], for which no signature existed.

3. Time critical operation - Some OT systems are time critical in their operation. A certain action must occur at a certain time, with any delay having knock on effects to later processes. Delays of milliseconds before a message is delivered has the potential to cause problems.

4. Downtime unacceptable - In ICT environments downtime for maintenance is acceptable. It can occur at times where it will cause the least inconvenience. In an OT environment, this is not true. The power grid cannot simply be taken down for five minutes, it is an essential service that is required 24/7.

5. Proprietary protocols - Observing TCP/IP networks is well understood: the structure of messages is known and documentation is freely available. Protocols used by older OT devices are often proprietary, for which limited or no documentation is made available by the manufacturer. Some of these protocols are no longer supported but are still used, due to the hardware remaining in service for decades. This can not only lead to no support from the vendor, but also a declining pool of expertise as staff who are familiar with the protocol retire or change jobs.

6. Airgapping - In the past, manufacturers of OT equipment recommended that their hardware should be airgapped: having no physical connection to the outside world. While a good idea in theory, airgapping is now considered impractical [67]. However, CNI owners may still abide by this concept and refuse any outside connections to the site.

To explore the feasibility of performing cyber OMR at CNI, we conducted practical exercises to determine what is possible with existing tools.

7.3. Exploring the practicalities

Performing research upon OT systems is challenging. As discussed, they are often fragile and have a zero-downtime requirement. CNI owners are understandably reluctant to allow researchers access to conduct experiments at critical sites. A common solution is to use simulations: using software to represent the hardware, software and protocols that would be in use at a real site. Simulations of OT systems have been developed by other researchers [68, 69], but are limited in their ability to reflect all of the properties of an operational deployment [70]. An alternative approach is to develop a test bed using the actual hardware and software found in critical national infrastructure. This approach brings benefits: a simulation can represent what hardware is supposed to do, actual hardware shows both documented and undocumented behaviour. The primary disadvantage in this approach is cost.

The OT test bed based at Airbus in Newport (Wales) is such a solution, and was made available to assist in our research. As part of Airbus' wider research into OT security, the testbed is used to explore new ways of protecting the core devices which run CNI and the team have a number of OT specific attacks to test novel defences. This made it a good choice for also testing how cyber peacekeepers could practically monitor for such attacks. Linking back to our scenario, the testbed's smart city was used to represent Country A's power grid. This is a model of a city, where the power supply is controlled by Allen Bradley controllers and the Ignition HMI software. The city is shown in figure 12.

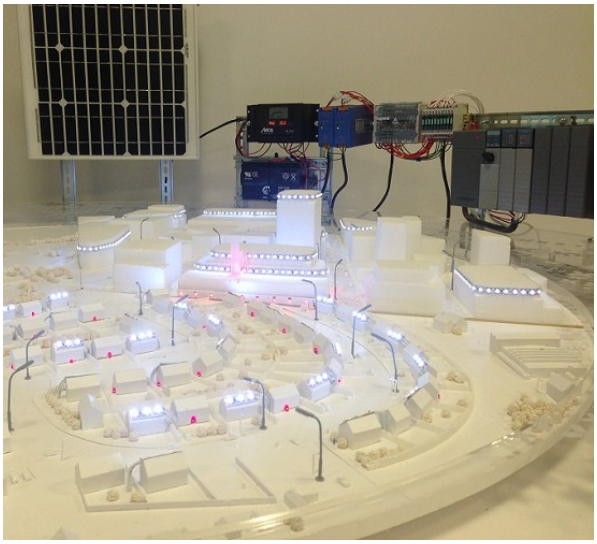

Figure 12: Airbus OT test bed city

To test traditional tools, an ICT based sensor was built (based upon Alienvault OSSIM) and added to the test bed. A free port was located on the network, and a mirror configured to forward traffic. While this was easy to accomplish in a test bed environment, it will be more complex in a live environment. Site operators may be suspicious of adding new devices to what may be a fragile system that has remained unchanged for years. Finding a physical connection into the network may be challenging, and connecting the sensor into a position where it can see traffic without interrupting or delaying communication will be an issue.

Once the sensor was in place, an attack was launched against the control system resulting in a loss of power to the city. The sensor did not raise any alerts during this attack. This was the expected result, since modules were designed to detect threats in ICT, not OT, environments. Other researchers have found similar results [71].

Commercial security product vendors have noticed this gap in the market, and a number of products are starting to enter the market for OT monitoring. For example, Check Point Software Technologies[72], Alienvault [73] and Claroty [74] advertise specialised OT security monitoring tools. Researchers have recently developed distributed intrusion detection system (DIDS) for SCADA systems [75]. Airbus itself has also developed a number of prototype solutions to address specific OT security issues, such as safe asset discovery and forensic investigation tools.

Looking wider, further possibilities include model-based detection [76]. Here the behaviour of an OT system is passively monitored for abnormalities in its operation. Researchers such as Nicholson, Janicke and Cau [77] have explored this, by examining the value of Interval Temporal Logic (ITL) as a method for observing the state of OT hardware and software systems at various points in time. They launched two attacks against a controller, and noted that ITL was successful in spotting that the state of the controller had changed. XSense from CyberX claims to leverage this approach using machine learning, modelling abilities and a patented state machine design [78]. The product requires a learning period, where normal operation is witnessed and recorded by the tool. In a cyber OMR context this "model based" approach may have limited utility; the ability to provide a period of learning in a "safe" state may be lacking if the site is already compromised before cyber peacekeepers arrive.

Any attempt to define specific tools or methods to conduct cyber OMR at CNI would be flawed: effective monitoring will depend upon the configuration of hardware, protocols and software at a specific site. Furthermore the quality and quantity of OT monitoring tools is advancing rapidly in this area and any recommendations would quickly become out of date. We therefore propose that cyber OMR at CNI will require a bespoke monitoring solution, where the expertise and knowledge of cyber peacekeepers is applied along with OT vendor collaboration. As an example, there are specific methods for monitoring power distribution sites such as the deployment of phasor measurement units (PMUs) to measure the actual voltage and other variables in real time [79, 80]. Such a solution was a major recommendation following the 2003 blackout in the northeastern United States [81] and will require specialist knowledge to implement.

8. Reporting

Previous sections have described how to perform cyber observation and monitoring. The aim of this section is to explore the practicalities of the final aspect: reporting. Reporting is just as important as the monitoring and observation that comes before it. We can gather all kinds of valuable observations, but that value is lost if they are not communicated properly and used in decision making.

UN peacekeeping doctrine states that reports should be "timely, accurate, clear and concise, substantiated with evaluations and assessments, to support higher commanders' decision-making" [38]. UN standard operating procedures for reporting are well documented [82], and as with all aspects of cyber peacekeeping, we aim to fit cyber into this existing process. In a UN peacekeeping operation reports flow up from the tactical level up to the strategic level, with various points in between for filtering and collation of data. Using our modified organisational structure from section 4.2, figure 13 shows how cyber fits into this existing system.

Peacekeepers in a cyber unit will submit reports to the Joint Operations Centre (JOC), which already collates and cross-references information coming in from all units. This allows the JOC to formulate a daily report, providing the component heads and leadership team with a coherent overview of the day's events at the tactical level.

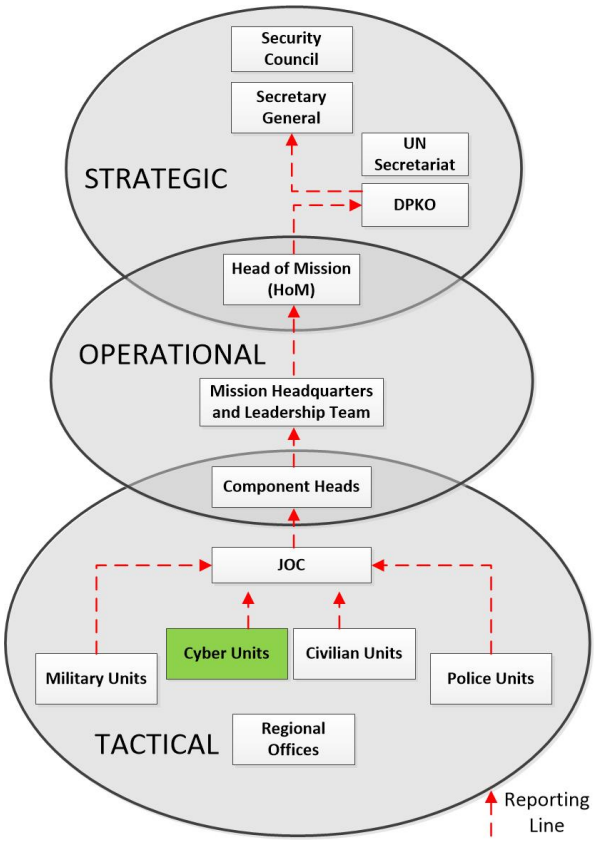

Figure 13: UN Operational Reporting System with Cyber added

In general, there are two types of reports that cyber peacekeepers performing OMR will need to submit: Daily SITREPS and Special Incident Reports. Cyber peacekeepers will be observing their AoR in order to detect and observe for a variety of events. Some of these events will be non-critical, such as a decline in cooperation from local staff or a non-malicious and non-critical repeat failure of a particular device at CNI. These events can be reported in the daily SITREP. This is a situation report which is submitted to the JOC on a daily basis, regardless of whether the peacekeeper considers there to have been any reportable events. The process of creating and forwarding daily SITREPS is well established in peacekeeping training material [82] and do not require any alterations for cyber. At the end of the day, cyber analysts based at the JOC meet with their team and convey their summary of cyber events for inclusion into the overall daily situation report sent to the operational level. Cyber peacekeepers are also observing for events which could lead to a threat to peace (e.g. to civilian life). In such cases it will be necessary for the event to be reported quickly. Here a special incident report (SINCREP) will be necessary, which is immediately submitted to the JOC for attention.

8.1. SINCREP Example

To provide a concrete example of our proposed system, we return to our scenario. Let us assume that the power plant AoR team detects unusual network activity on the power plant's control network. Abnormal messages are being sent to logic controllers, but peacekeepers at this stage are not sure what the effect will be. They generate a SINCREP which communicates their observations. They include the time the unusual activity first started, that it is ongoing, the IP addresses and hardware involved, a description of what is happening and the network capture files as evidence. This report is sent to the JOC and received by cyber staff. They analyse the report and view the evidence, entering into the virtual environment to communicate with the reporting peacekeepers in real-time. Because the JOC is collecting reports from all components, the cyber staff notice that a SINCREP is received from a police unit that power was briefly lost in a certain region. Putting these reports together to form a picture of the whole situation, the JOC is able to provide advance warning to other components that blackouts might be imminent around the region. The JOC then acts as a crisis centre to monitor the situation, inform relevant stakeholders, whilst the cyber peacekeepers continue to monitor the event and provide advice to local staff on defensive measures to take.

This scenario brings to the fore a significant question: should peacekeepers performing cyber OMR stand by and simply monitor and report whilst a situation degrades and threatens civilians, or should they actively intervene? This is not a new question faced by peacekeeping, and has undergone much discussion and debate [83, 84, 85]. Many past criticisms of UN peacekeeping have touched upon either the inability or unwillingness of peacekeepers to use force to protect civilians around them. UN Resolution 1265 (1999) emphasised the importance of protecting civilians during peace operations. Many missions have subsequently been established with a specific mandate to protect civilians from harm, using robust measures and loosening up use of force controls. This has led to the UN moving away from traditional doctrine, the Brahimi report and

core principles in favour of more robustly protecting civilians [86, 87].

With this shift of focus in mind, we will not attempt to state that a cyber peacekeeper performing OMR at a critical site should passively observe as a threat to civilian security materialises. Such an act would arguably be a repeat of past failures such as Bosnia [88] or Rwanda [89]. It is therefore accepted that when faced with an event where there is potential for harm to civilians, cyber peacekeepers should take any reasonable steps to prevent that harm if they are able to. The impacts of this decision will be further considered in the evaluation.

8.2. Integration with the VCE

Since we have proposed that a virtual environment will be central to cyber peacekeeping, it is prudent to explore the possibility of integrating the reporting system into it. The goal is to have as many tools as possible to perform cyber OMR in one unified location.

As a proof of concept, we used the RequestTracker [90] ticket system. This software allows immediate transmission and handling of reports, fulfilling the requirement that reports are timely. Custom fields were added to the ticket interface, with the aim of ensuring that tickets fulfilled the requirement for reports to be concise. The following fields were added:

- Start time of event.
- Type of event.
- Supporting evidence.
- AoR the event was detected in.
- The sensor which detected the event.

Some further modifications were made, with the end result being a proof of concept cyber OMR reporting system. The next goal was to examine how the ticket is managed post-creation. To define a set of rules regarding ticket states for cyber OMR, it was first necessary to develop the life cycle of a cyber peacekeeping OMR ticket. The proposed life cycle is presented visually in figure 14.

It was found that the ticket system integrated well into the VCE. Reports could be written inside the environment, allowing multiple actors to contribute to the content. An example is shown in figure 15.

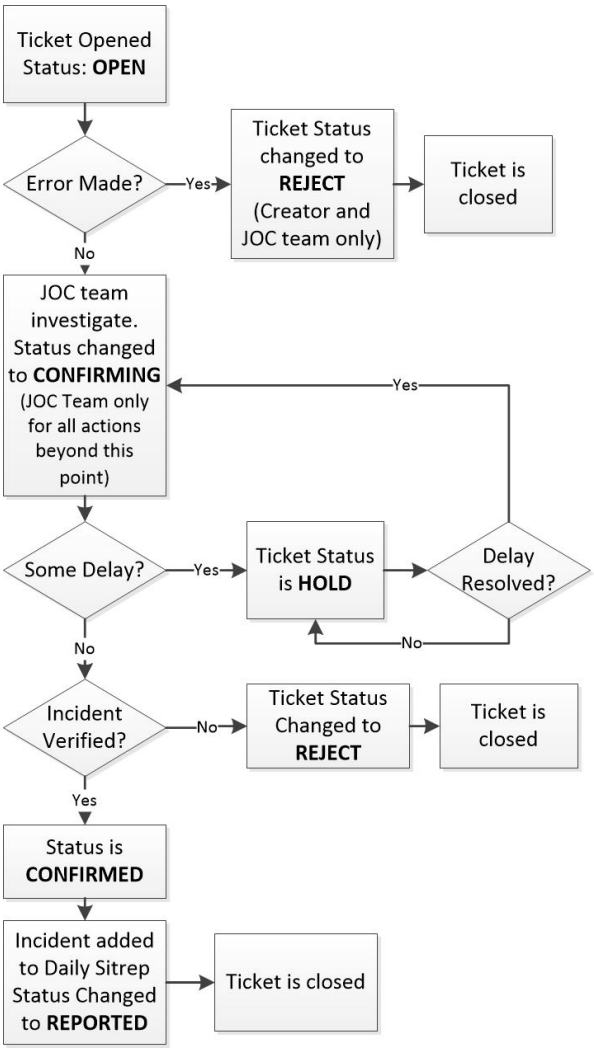

Figure 14: Proposed Cyber OMR Ticket Lifecycle

9. Evaluation of Cyber OMR against UN Peacekeeping Principles

In this paper, we have explored practical ways in which cyber OMR could be performed. We now evaluate our proposals against the core UN peacekeeping principles of consent, impartiality and non-use of force except in self defence or defence of the mandate.

9.1. Consent

UN peacekeeping doctrine [13] states that consent of the parties is one of the core UN principles. It is thus necessary to ensure that cyber OMR as we have designed it does not have the potential to violate this principle.

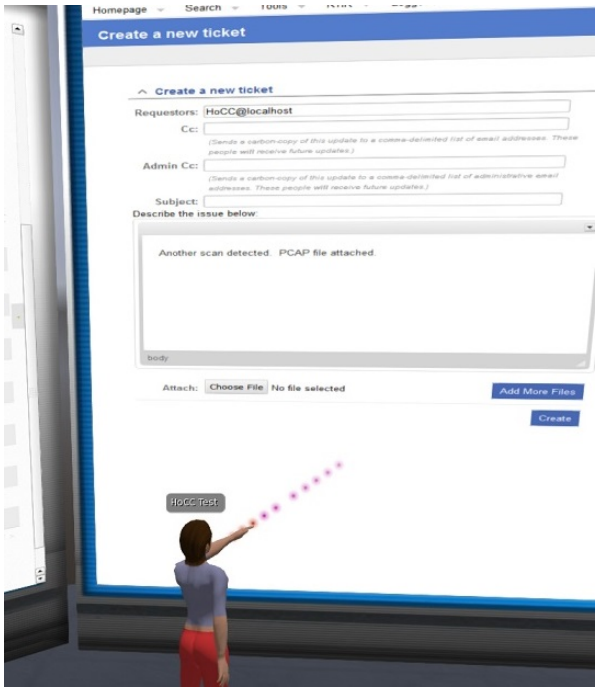

Figure 15: Interacting with RT from within the VCE

In our idealistic scenario, the presence of consent is clear. Both parties have requested UN assistance in overseeing the cyber warfare aspect of the peace agreement, and both sides have invited the UN to monitor certain critical sites. Consent in this case is not only respected, but we would argue fundamentally required. Attempting to install sensors, gain familiarity with sites and keep the system running is only possible by working closely with local staff. If local staff are not cooperative or work against cyber peacekeepers, cyber peacekeeping OMR will be extremely challenging to perform effectively. Consent is the reason why some observational goals were deemed to be low feasibility. For example, monitoring for violations of privacy. If a host nation is snooping upon its citizens in the cyber domain, they are unlikely to consent to cyber peacekeeping if it was believed that cyber peacekeepers were looking to criticise privacy violations. Therefore, the principle of consent leads to such activities not being included at this stage. It is not worth blocking the value that cyber OMR can bring in regards to protecting civilian lives, for the sake of attempting to also protect their privacy.

It is foreseeable that there will be cases where the principle of consent can become threatened. For example, peacekeepers performing cyber OMR at sites such as nuclear plants or dams could face a situation where a significant threat to civilian life has been detected but local staff refuse and resist corrective action to prevent it. This will be a problem, since it is made clear in UN peacekeeping doctrine that peacekeepers must not stand by and remain passive in the face of clear threats to civilians [91]. We have already proposed that a cyber peacekeeper should not stand by and passively observe while an event escalates to a level where civilian life is threatened.

In such cases, there is strong justification for intervention without consent: effectively a step into peace enforcement. How this could be done remains an open question, and it could have significant negative effects such as a withdrawal of consent for the whole peace operation. Planning could minimise the likelihood of this risk. For example, parties requesting cyber OMR must agree at the outset that threats to civilian life must be acted upon by local staff, and that interventions may take place if cooperation at these times is lacking. By making parties aware of this, the effects of these interventions can be minimised to not endanger the whole peace process. Drills of a crisis situation could be valuable, to gauge how local staff react and highlight any potential issues before they arise.

A further complication to consent is the area of public versus private ownership. While kinetic OMR primarily takes place in the public domain (observing roads, bridges, towns etc.), cyber OMR has the potential to be taking place in privately owned networks. For example, a nuclear power plant may be owned by a foreign energy company. This means that whilst kinetic OMR can function purely with the consent of a national government (the owners of these public spaces), cyber OMR will potentially require the consent of both public and private entities. This is an interesting area to consider and must form a suggestion for future work.

Finally, whilst our scenario represents an ideal scenario from the perspective of gaining consent, the reality of peacekeeping is often less clear. As noted by de Coning [86] peace operations today have been noted for their lack of clear consent, with the Security Council issuing a mandate against a specific party to the conflict. If our scenario changed so that Country B did not provide consent, the task of performing cyber OMR in that country would become much more challenging.

9.2. Impartiality

The principle of impartiality is important to UN peacekeeping, ensuring that peacekeepers can act as a trusted party. In our scenario, impartiality is respected. Both sides are offered cyber OMR, and peacekeepers are not attempting to attribute cyber attacks to a particular side.

Cyber OMR must be offered to all parties of a conflict equally. If it appears that the UN is providing cyber OMR for a number of sites in Country A and that Country B is not offered the same opportunity, there is potential for the principle of impartiality to be violated. It should therefore be made clear to parties at the outset that cyber OMR is available to all, but that only a limited number of sites will be monitored based upon the potential threat to civilian security.

A threat to impartiality is found in resource contention. One party may request cyber OMR at twenty sites, consuming the majority of UN cyber peacekeeping resources. If another party makes a similar request a month later, the UN may find itself unable to fulfil the request and impartiality will again be violated. Peacekeepers must be conservative when agreeing to monitoring, and only agree to sites where failure could lead to civilians being harmed or another threat to peace, such as state collapse. The focus of cyber OMR must clearly be one of these goals, not to provide "free" security monitoring so that a party can divert their own cyber resources elsewhere.

Cyber OMR teams must also make efforts to be transparent in the tasks they perform, to avoid claims that cyber peacekeepers are helping one party more than the other. Considering our proposal that cyber peacekeepers must intervene if they can prevent a threat to civilians, this will be challenging. Our virtual collaborative environment presents opportunities here, with the potential for stakeholders from both sides to have a presence in the environment and witness the tasks that cyber peacekeepers perform. This would enhance transparency, and help to minimise claims of partiality.

9.3. Non use of force

Our design of cyber OMR does not utilise force. Attacks against an AoR are observed and reported through the reporting system. Cyber peacekeepers are not attempting to take offensive actions such as launching counter cyber attacks. Although OMR is primarily passive, it was noted that peacekeepers are required to intervene if a grave violation of human rights is observed. This equates to a situation such as a cyber attack which is close to opening a dam or making the public water supply toxic. In such scenarios, cyber peacekeepers must intervene if possible to prevent the harm. This intervention will likely be through notifying the network owner, advising them on what must be done and assisting with implementing the action. Such an action would not be a use of force. In cases where the response from the network owner is lacking, local cyber peacekeepers may have to take enforcement action. If the local staff actively resist, there is a situation where force could be the next step. This would require cyber units to be supported by police or military units to provide physical security whilst the action is taken. In such a scenario, the use of force would be in defence of the mandate. It would therefore not violate the principle.

10. Conclusions and Future Work

In this paper, we have explored the practicalities of starting up and performing just one cyber peacekeeping activity: cyber OMR. Basing our work on the foundations set in previous work [4] we have reached a number of conclusions, summarised below:

- Cyber terms in peace agreements should be chosen carefully. We want to avoid terms which require solid attribution in cyberspace, and favour those which can be measured at a human interaction level while still bringing value.
- Securing the required cyber expertise will likely be the biggest obstacle towards cyber peacekeeping.
- Cyber fits easily into existing structures and processes.
- Cyber OMR will bring most value at CNI, with a focus on protection of civilians and state stability.
- Technical obstacles towards monitoring CNI are being broken down as new products and tools come to market, but there is still a skills shortage in this area, which will place further pressure on securing capable staff.

- Use of a virtual collaborative environment brings a number of benefits including transparency, ease of collaboration, information sharing and the potential for states to contribute their cyber experts without losing capability at home.
- Our proposals do not violate established UN peacekeeping principles.

The discussions held in this paper raise deeper questions about cyber OMR as an activity. Firstly, UN peacekeeping as a whole is currently undergoing a shift in how it operates. The doctrine we have based our scenario on is the 2008 capstone [13]. This is the current 'official' way in which UN peacekeeping should work, based upon the findings of the Brahami report [91]. However, many authors point out that UN peace operations of today do not follow this doctrine [86, 92]. For example, in the DRC consent from all parties is not present, with some openly hostile to peacekeeping forces. Neither is impartiality, with the UN effectively supporting a government against insurgency. Non use of force is also questionable, with the UN actively partaking in offensive operations in collaboration with government forces [86]. It would therefore be useful to present a scenario which does not fit the 2008 doctrine and explore the impact upon the value and feasibility of cyber OMR.

We proposed that a peacekeeper performing cyber OMR must intervene to prevent harm if they are able to do so. This raises a question about the role of cyber OMR as a passive activity. If cyber peacekeepers are commonly stepping in to take action, it is arguably more efficient to establish a cyber buffer zone from the outset. In this regard, it is possible to propose that cyber OMR should not be a standalone activity, but rather a component of a cyber buffer zone. This will be explored in future work regarding cyber buffer zones.

An area of future work is to look at feasible ways of solving the challenge of securing cyber expertise. If the major obstacle towards effective cyber OMR will be the limited supply of cyber expertise and political concerns from highly developed nations (as discussed in section 4.1), it would be prudent to explore non-UN means of protecting civilians and state stability both during and following cyber warfare. For example, alliances such as NATO or the Arab League where the member states share common military goals and would be more willing to share cyber expertise.

It would also be valuable to explore how existing frameworks could be leveraged to bolster cyber OMR. Many initiatives are under way in a number of countries [93, 94]. For example, the NIS Directive in Europe demands that member states have in place a framework and national cyber security authority (NCSA) so that they are equipped to manage cyber security incidents [95, 96]. These NCSAs would likely be major enablers and contributors to cyber peacekeeping, allowing peacekeepers to quickly enter sites and gain familiarity. Operators of essential services also have to take appropriate security measures and are required to report cyber security incidents. In this regard, it could be argued that frameworks such as the NIS Directive already go some way to motivating owners of critical infrastructure to develop a monitoring capability. From a cyber peacekeeping perspective, efforts such as NIS could reduce the initial workload to establish a monitoring capability in a nation.

Finally, this article has only sought to develop the peacekeeping activity of cyber OMR. As described in Robinson et al. [4], there are many more valuble and feasible activities which need further development. Developing activities such as DDR, SSR, malware action and the practicalities of cyber ceasefire agreements remains an open area of work. Input from experts in these areas is essential, since cyber peacekeeping is fundamentally a cross disciplinary challenge. Furthermore, other forms of peace operations such as conflict prevention and peace enforcement also remain open. Conflict prevention in particular has been regarded as critical towards the future of peace operations [97]. It would therefore be valuable to explore efforts such as the confidence building measures put forward by the OSCE [98] and other groups.

References

[1] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Computers & Security*, vol. 49, pp. 70 – 94, 2015.

[2] T. Cahill, K. Rozinov, and C. Mule, "Cyber warfare peacekeeping," in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pp. 100–106, June 2003.

[3] N. Akatyev and J. I. James, *Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. Revised Selected Papers*, ch. Cyber Peacekeeping, pp. 126–139. Springer International Publishing, 2015.

[4] M. Robinson, K. Jones, H. Janicke, and L. Maglaras, "An introduction to cyber peacekeeping," *Journal of*

Network and Computer Applications, vol. 114, pp. 70 – 87, 2018.

[5] M. Akebo, *Ceasefire Agreements and Peace Processes*. Routledge, 2016.

[6] C. Johnson, "Peacemaking and peacekeeping: Reflections from abyei," *International Peacekeeping*, vol. 19, no. 5, pp. 640–654, 2012.

[7] Public International Law & Policy Group, *The Ceasefire Drafter's Handbook*. 2013.

[8] A. Cook, A. Nicholson, H. Janicke, L. Maglaras, and R. Smith, "Attribution of cyber attacks on industrial control systems," *Industrial Networks and Intelligent Systems*, 2016.

[9] M. N. Schmitt and L. Vihul, "Proxy wars in cyber space: The evolving international law of attribution," *Fletcher Security Review*, vol. 1, no. 2, pp. 55–73, 2014.

[10] H. Berghel, "On the problem of (cyber) attribution," *IEEE Computer*, vol. 50, no. 3, pp. 84–89, 2017.

[11] N. Haysom and J. Hottinger, "Do's and don'ts of sustainable ceasefire agreements," 2004. Presentation revised for use by Peace Appeal in Nepal and Sri Lanka.

[12] United Nations, "Handbook on United Nations Multidimensional Peacekeeping Operations," December 2003.

[13] United Nations, "United Nations Peacekeeping Operations: Capstone Doctrine," January 2008.

[14] United Nations, "Global peacekeeping data," Feb. 2018. `https://peacekeeping.un.org/en/data`, accessed 13/04/2018.

[15] United Nations, "How we are funded," 2018. `https://peacekeeping.un.org/en/how-we-are-funded`, accessed 18/04/2018.

[16] A. Bellamy and P. Williams, *Providing Peacekeepers: The Politics, Challenges, and Future of United Nations Peacekeeping Contributions*. OUP Oxford, 2013.

[17] W. Zhengyu and I. Taylor, "From refusal to engagement: Chinese contributions to peacekeeping in africa," *Journal of Contemporary African Studies*, vol. 29, no. 2, pp. 137–154, 2011.

[18] V. Bove and L. Elia, "Supplying peace: Participation in and troop contribution to peacekeeping missions," *Journal of Peace Research*, vol. 48, no. 6, pp. 699–714, 2011.

[19] United Nations, "Civilians," Apr. 2018. `https://peacekeeping.un.org/en/civilians`, accessed 05/03/2018.

[20] J. Elsea, M. Schwartz, and K. Nakamura, *Private Security Contractors in Iraq: Background, Legal Status, and Other Issues*. Library of Congress, 2008.

[21] A. Bellamy and P. Williams, "The West and Contemporary Peace Operations," *Journal of Peace Research*, vol. 46, no. 1, pp. 39–57, 2009.

[22] N. Serafino, "Policing in peacekeeping and related stability operations: Problems and proposed solutions," 2004. `http://www.dtic.mil/dtic/tr/fulltext/u2/a465324.pdf`, accessed 20/06/2018.

[23] W. J. Durch, V. K. Holt, C. R. Earle, and M. K. Shanahan, "The brahimi report and the future of un peace operations," tech. rep., Stimson Center, 2003.

[24] A. Sternstein, "US Cyber Command Has Just Half the Staff It Needs," *DefenceOne*, February 2015.

[25] M. Libicki, "Checklist for a U.S.-Russia Cyberwar," *RAND Corporation*, 2016.

[26] S. Shaikh, "If Russia launches a cyber attack on the UK, this is what we can do," *The Independent*, April 2018. `https://www.independent.co.uk/voices/russia-cyber-war-nerve-agent-may-defense-warfare-a8307391.html`, accessed 20/06/2018.

[27] R. C. Thakur, C. Aoi, and C. De Coning, *Unintended consequences of peacekeeping operations*. United Nations University Press, 2007.

[28] L. Heinecken and R. Ferreira, "Fighting for peace: The psychological effect of peace operations on south african peacekeepers," *African Security Review*, vol. 21, no. 2, pp. 50–60, 2012.

[29] Y. Loscalzo, M. Giannini, A. Gori, and A. D. Fabio, "The wellbeing of italian peacekeeper military: Psychological resources, quality of life and internalizing symptoms," *Frontiers in psychology*, vol. 9, p. 103, 2018.

[30] UN Department of Peacekeeping Operations, *Integrated Assessment and Planning (IAP) Handbook*. United Nations, 2013.

[31] A. Boutellis, *Driving the System Apart?: A Study of United Nations Integration and Integrated Strategic Planning*. 2013.

[32] United Nations DPKO, *Planning Toolkit*. United Nations, 2014.

[33] United Nations, *United Nations Infantry Battalion Manual Volume 1*. United Nations, August 2012.

[34] R. Bejtlich, *The Practice of Network Security Monitoring*. No Starch Inc., 2013.

[35] M. Collins, *Network Security Through Data Analysis*. Shroff Publishers & Distr, 2014.

[36] C. Sanders and J. Smith, *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Syngress Publishing, 1st ed., 2013.

[37] C. Sanders, *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*. San Francisco, CA, USA: No Starch Press, 3rd ed., 2017.

[38] United Nations, *United Nations Infantry Battalion Manual Volume 2*. United Nations, August 2012.

[39] L. Cherbakov, R. Brunner, R. Smart, and C. Lu, "Virtual spaces: Enabling immersive collaborative enterprise." IBM, June 2009.

[40] S. Redfern and N. Naughton, "Collaborative virtual environments to support communication and community in internet-based distance education," *Journal of Information Technology Education*, vol. 1, no. 3, 2002.

[41] X. Zhang and G. W. Furnas, "The effectiveness of multiscale collaboration in virtual environments," in *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '03, (New York, NY, USA), pp. 790–791, ACM, 2003.

[42] C. Bouras, E. Giannaka, and T. Tsiatsos, "Virtual collaboration spaces: the eve community," in *Applications and the Internet, 2003. Proceedings. 2003 Symposium on*, pp. 48–55, Jan 2003.

[43] S. Ahma-aho and T. Surakka, "Benchmark of 3D virtual environments," 2011. `https://blogs.aalto.fi/allthingsvirtual/files/2011/06/Benchmark_Report1.pdf`, Accessed 20/06/2018.

[44] Unity Technologies, "Unity3d website," May 2018. `https://unity3d.com/`, accessed 17/04/2018.

[45] OpenVCE, "Open Virtual Collaboration Environment Website," 2015. `http://openvce.net`, accessed 02/02/2018.

[46] R. Bejtlich, *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley Professional, 2004.

[47] D. Donald, "Neutrality, impartiality and un peacekeeping at the beginning of the 21st century," *International Peacekeeping*, vol. 9, no. 4, pp. 21–38, 2002.

[48] A. Jøsang, "Potential cyber warfare capabilities of major technology vendors," in *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece*, p. 110, 2014.

[49] A. Chakrabarti and G. Manimaran, "Internet infrastructure security: A taxonomy," *IEEE network*, vol. 16, no. 6, pp. 13–21, 2002.

[50] Immarsat, "Immarsat BGAN Service Website," 2017. `http://www.inmarsat.com/service/bgan/`, accessed 21/03/2018.

[51] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55 – 82, 2018.

[52] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems," *Technovation*, vol. 34, no. 7, pp. 342–353, 2014.

[53] Cisco, "Introduction to Cisco IOS NetFlow (Whitepaper)," 2012. `https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html`, accessed 20/02/2018.

[54] UK Centre for the Protection of National Infrastructure, ""The National Infrastructure"," May 2018. `https://www.cpni.gov.uk/critical-national-infrastructure-0`, Accessed 15/06/2018.

[55] M. Robinson, "The scada threat landscape," in *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013*, ICS-CSR 2013, (UK), pp. 30–41, BCS, 2013.

[56] P. Cornish, D. Livingstone, C. Yorke, and D. Clemente, *Cyber Security and Critical National Infrastructure: Chatham House Report*. Royal Inst of Intl Affairs, 2012.

[57] M. Rudner, "Cyber-threats to critical national infrastructure: An intelligence challenge," *International Journal of Intelligence and CounterIntelligence*, vol. 26, no. 3, pp. 453–481, 2013.

[58] A. Cook, R. Smith, L. Maglaras, and H. Janicke, "Using gamification to raise awareness of cyber threats to critical national infrastructure," BCS, 2016.

[59] R. Piggin, "Industrial systems: cyber-security's new battlefront [information technology operational technology]," *Engineering Technology*, vol. 9, pp. 70–74, Sept 2014.

[60] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *International journal of critical infrastructure protection*, vol. 8, pp. 53–66, 2015.

[61] A. R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, June 2015.

[62] L. M. Zeichner, "Developing an overarching legal framework for critical service delivery in america's cities: Three recommendations for enhancing security and reliability," *Government Information Quarterly*, vol. 18, no. 4, pp. 279 – 291, 2001.

[63] K. Quigley, C. Burns, and K. Stallard, "Cyber gurus: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection," *Government Information Quarterly*, vol. 32, no. 2, pp. 108 – 117, 2015.

[64] M. Merabti, M. Kennedy, and W. Hurst, "Critical infrastructure protection: A 21 st century challenge," in *Communications and Information Technology (ICCIT), 2011 International Conference on*, pp. 1–6, IEEE, 2011.

[65] A. Wedgbury and K. Jones, "Automated asset discovery in industrial control systems - exploring the problem," in *3rd International Symposium for ICS & SCADA Cyber Security Research*, 2015.

[66] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, pp. 48–53, Februrary 2013.

[67] E. Byres, "The Air Gap: SCADA's Enduring Security Myth," *Commun. ACM*, vol. 56, pp. 29–31, August 2013.

[68] C. Queiroz, A. Mahmood, and Z. Tari, "Scadasim - a framework for building scada simulations," *IEEE Transactions on Smart Grid*, vol. 2, pp. 589–597, Dec 2011.

[69] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (tasscs)," in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, pp. 1–7, Jan 2011.

[70] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar, and M. Higdon, "Development of the powercyber scada security testbed," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, CSIIRW '10, (New York, NY, USA), pp. 21:1–21:4, ACM, 2010.

[71] A. Mahboob and J. Zubairi, "Securing scada systems with open source software," in *High Capacity Optical Networks and Enabling Technologies, 10th International Conference on*, pp. 193–198, 2013.

[72] Check Point Software Technologies LTD, "Critical Infrastructure & ICS/SCADA," 2016. `http://www.checkpoint.com/products-solutions/critical-infrastructure/`, Accessed 19/06/2018.

[73] Alienvault, "SCADA Security for Energy and Utility Companies," 2018. `https://www.alienvault.com/solutions/scada-security`, Accessed 02/03/2018.

[74] Claroty LTD, "Claroty Website," 2018. `https://www.claroty.com/`, accessed 07/04/2018.

[75] T. Cruz, L. Rosa, J. Proença, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, and P. Simões, "A cybersecurity detection framework for supervisory control and data acquisition systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2236–2246, 2016.

[76] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for scada networks," in *Proceedings of the SCADA Security Scientific Symposium*, (Miami Beach, Florida), Jan. 2007.

[77] A. Nicholson, H. Janicke, and A. Cau, "Position paper: Safety and security monitoring in ics/scada systems," in *2nd International Symposium for ICS & SCADA Cyber Security Research*, 2014.

[78] Cyber X, "X Sense Website," 2017. `https://cyberx-labs.com/en/xsense/`, accessed 15/05/2018.

[79] J. Eto, E. Stewart, T. Smith, M. Buckner, H. Kirkham, F. Tuffner, and D. Schoenwald, "Scoping study on research and priorities for distribution-system phasor measurement units," *Lawrence Berkeley National Laboratory*, 2015.

[80] M. Jamei, E. Stewart, S. Peisert, A. Scaglione, C. McParland, C. Roberts, and A. McEachern, "Micro synchrophasor-based intrusion detection in automated distribution systems: Toward critical infrastructure security," *IEEE Internet Computing*, vol. 20, no. 5,

pp. 18–27, 2016.
[81] B. Liscouski and W. Elliot, "Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations," *A report to US Department of Energy*, vol. 40, no. 4, 2004.
[82] United Nations, *UN Peacekeeping PDT Standards, Specialized Training Material for Military Experts on Mission 1st Edition 2010*. 1 ed., 2010.
[83] C. Ryngaert and N. Schrijver, "Lessons learned from the srebrenica massacre: From un peacekeeping reform to legal responsibility," *Netherlands International Law Review*, vol. 62, pp. 219–227, Jul 2015.
[84] S. Wills, *Protecting civilians: the obligations of peacekeepers*. Oxford University Press, 2009.
[85] UN General Assembly, "Evaluation of the implementation and results of protection of civilians mandates in united nations peacekeeping operations a/68/787," March 2014.
[86] C. de Coning, J. Karlsrud, and C. Aoi, eds., *UN Peacekeeping Doctrine in a New Era: Adapting to Stabilisation, Protection and New Threats*. Routledge, 2017.
[87] J. Ramos-Horta *et al.*, "Uniting our strengths for peace–politics, partnership and people: Report of the high-level independent panel on united nations peace operations," *New York: United Nations (16 June)*, 2015.
[88] R. Hanlon and K. Christie, *Freedom from Fear, Freedom from Want: An Introduction to Human Security*. Toronto University Press, 2016.
[89] M. N. Barnett, "Peacekeeping, indifference, and genocide in rwanda," *Cultures of Insecurity: States, Communities, and the Production of Danger*, vol. 14, p. 173, 1999.
[90] Best Practical, "RT: Request Tracker Website," 2018. `http://bestpractical.squarespace.com/request-tracker`, accessed 20/06/2018.
[91] United Nations, General Assembly, "Comprehensive review of the whole question of peacekeeping operations in all their aspects A/55/305," 2000.
[92] P. Mateja, "Between doctrine and practice: The un peacekeeping dilemma," *Global Governance: A Review of Multilateralism and International Organizations*, vol. 21, no. 3, pp. 351–370, 2015.
[93] J. Ruohonen, S. Hyrynsalmi, and V. Leppnen, "An outlook on the institutional evolution of the european union cyber security apparatus," *Government Information Quarterly*, vol. 33, no. 4, pp. 746 – 756, 2016.
[94] N. Choucri, S. Madnick, and J. Ferwerda, "Institutions for cyber security: International responses and global imperatives," *Information Technology for Development*, vol. 20, no. 2, pp. 96–121, 2014.
[95] L. Maglaras, G. Drivas, K. Noou, and S. Rallis, "Nis directive: The case of greece," *EAI Endorsed Transactions on Security and Safety*, vol. 18, 5 2018.
[96] R. Piggin, "Nis directive and the security of critical services," *ITNOW*, vol. 60, no. 1, pp. 44–44, 2018.
[97] K. Annan, "Prevention of armed conflict (a/55/985-s/2001/574)," June 2001. `http://unpan1.un.org/intradoc/groups/public/documents/un/unpan005902.pdf`, Accessed 20/06/2018.
[98] Organization for Security and Co-operation in Europe, "Permanent council decision no. 1202," 2016. `https://www.osce.org/pc/227281`, Accessed 12/05/2018.